2100

2131

Practitioner's Docket No. 41230/55769

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: J. Hoffstein et al.

Application No.: 09/939,531 Group No.:
Filed: 08/24/01 Examiner:

Assistant Commissioner for Patents
Washington, D.C. 20231

TRANSMITTAL OF INFORMATION DISCLOSURE STATEMENT WITHIN THREE MONTHS OF FILING OR BEFORE MAILING OF FIRST OFFICE ACTION (37 C.F.R. SECTION 1.97(b))

NOTE: "An information disclosure statement shall be considered by the Office if filed by the applicant: (1) within three months of the filing date of a national application; (2) within three months of the date of entry of the national stage as set forth in section 1.491 in an international application; or (3) before the mailing date of a first Office action on the merits, whichever event occurs last." 37 C.F.R. section 1.97(b).

NOTE: The "filing date of a national application" under 37 C.F.R. section 1.97(b) has two possible meanings. Where the filing is a direct one to the United States Patent & Trademark office, the filing is defined in 37 C.F.R. section 1.53(b) as "the date on which: (1) A specification containing a description pursuant to section 1.71 and at least one claim pursuant to section 1.75; and (2) any drawing required by section 1.81(a), are filed in the Patent and Trademark Office in the name of the actual inventor or inventors as required by section 1.41." 37 C.F.R. section 1.97(b)(1). On the other hand, an international application that enters the national stage occurs when the applicant has filed the documents and fees required by 35 U.S.C. section 371(c) within the periods set forth in section 1.494 or section 1.495. 35 U.S.C. section 371(c) requires the filing of the following: (1) the basic national fee; (2) a copy of the international application, unless already sent by the International Bureau, and optionally an English translation if filed in another language; and, also optionally (3) amendments under PCT Article 19, with a translation into English if made in another language; (4) an oath or declaration; and (5) a translation into English of any annexes to the international preliminary examination report, if such annexes were made in another language. The optional items must be submitted later, with surcharges. 37 C.F.R. section 1.97(b)(2).

IDENTIFICATION OF TIME OF FILING THE ACCOMPANYING INFORMATION DISCLOSURE STATEMENT

The information disclosure statement submitted herewith is being filed within three months of the filing date of the application or date of entry into the national stage of an international application or before the mailing date of a first Office action on the merits, whichever event occurs last. 37 C.F.R. section 1.97(b).

NOTE: "No certification or fee is due when the filing is made within the above time period. It is advisable to ensure that no

Office action has been mailed if the disclosure statement is delayed until after three months from filing."

NOTE: *"An information disclosure statement will be considered to have been filed on the day it was received in the Office, or on an earlier date of a mailing if accompanied by a properly executed certificate of mailing under 37 C.F.R. 1.8, or Express Mail certificate under 37 C.F.R. 1.10. An office action is mailed on the date indicated in the Office action." Notice of April 20, 1992 (1138 O.G. 37-41, 39).*

NOTE: *"The term 'national application' includes continuing applications (continuations, divisions, continuations-in-part) so three-months will be measured from the actual filing date of an application as opposed [sic] to the effective date of a continuing application." Notice of April 20, 1992 (1138 O.G. 37-41, 39).*

NOTE: *"An action on the merits means an action which treats the patentability of the claims in an application, as opposed to only formal or procedural requirements. An action on the merits would, for example, contain a rejection or indication of allowability of a claim or claims rather than just a restriction requirements (37 C.F.R. section 1.142) or just a requirement for additional fees to have a claim considered (37 C.F.R. section 1.16(d)). Thus, if an application was filed on Jan. 1 and the first Office action on the merits was not mailed until six months later on July 1, the examiner would be required to consider any proper information disclosure statement filed prior to July 1." Notice of April 20, 1992 (1138 O.G. 37-41, 39).*

WARNING: *"A petition for suspension of action to allow applicant time to submit an information disclosure statement will be denied as failing to present good and sufficient reasons, since 37 C.F.R. section 1.97 provides adequate recourse for the timely submission of prior art for consideration by the examiner." Notice of July 6, 1992 (1141 O.G. 63).*

Cara Z. Lowen

SIGNATURE OF PRACTITIONER

Reg. No. 38,227

Cara Z. Lowen
(type or print name of practitioner)
DIKE, BRONSTEIN, ROBERTS & CUSHMAN
Intellectual Property Group of
EDWARDS & ANGELL, LLP.
P.O. Box 9169
Boston, MA 02209
Tel: (617) 439-4444

Customer No. 21874

BOS2_178862.2

FORM PTO-1449	DOCKET NO:	SERIAL NO.:
	41230/55769	09/939,531
INFORMATION DISCLOSURE STATEMENT	APPLICANT(S): J. Hoffstein et al.	
	FILING DATE: August 24, 2001	GROUP NO.:

UNITED STATES PATENT DOCUMENTS

EXAM. INITIALS		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE

FOREIGN PATENT DOCUMENTS

		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION YES/NO
	BA						
	BB						

OTHER DOCUMENTS (INCLUDING AUTHOR, TITLE, DATE, PERTINENT PAGES, ETC.)

	CA	Con Coppersmith and Gadiel Seroussi, On the Minimum Distance of Some Quadratic Residue Codes, IEEE Transactions on Information Theory, Vol. IT-30 No. 2 March 1984, pp. 407-411,
	CB	Finite Field and Elliptic Curve Systems, Stinson Cryptography Theory and Practice, pp. 177-190
	CC	Jerome A. Solinas, Designs, Codes and Cryptography, 19, 195-249 (2000), Efficient Arithmetic on Koblitz Curves, , pp. 125-179
	CD	Chapter 14 Exponentiation, Menezen Van Oorschot and Vanstone, Handbook of Applied Cryptography, pp. 613-628
	CE	The Powering Algorithms, Henri Cohen, A Course in Computational Number Theory, pp. 8-12
	CF	Chae Hoon Lim et al., Sparse RSA Secret Keys and Their Generation, pp. 1-15. (preprint)
	CG	D.R. Stinson, Some Baby-step giant-step algorithms for the low hamming weight discrete logarithm problem, , pp. 1-15
	CH	What is a Random Sequence?, pp 149-179
	CI	Evaluation of Powers, pp. 461-481.
	CJ	Darrel Hankerson, Software Implementation of Elliptic Curve Cryptography over Binary Fields, pp. 1-24. (2000)

FORM PTO-1449	DOCKET NO:	SERIAL NO.:
INFORMATION DISCLOSURE STATEMENT	41230/55769	09/939,531
	APPLICANT(S): J. Hoffstein et al.	
	FILING DATE: August 24, 2001	GROUP NO.:

	CK	Jeffrey Hoffstein, NTRU: A Ring-Based Public Key Cryptosystem, et al. pp. 268-288
	CL	Peter de Rooij, On the Security of the Schnorr Scheme Using Preprocessing, Eurocrypt, pp. 71-80, (1998)
	CM	C.P. Schnorr, Efficient Identification and Signatures for Smart Cards, pp. 239-252, (1998)
	CN	Jeffrey Hoffstein, NSS: An NTRU Lattice-Based Signature Scheme
	CO	Daniel M. Gordon, A Survey of Fast Exponentiation Methods, December, 1997, Journal of Algorithms 27 (1998), 129-146, pp. 1-22

EXAMINER:	DATE:

GWN/rej